Auditoria de Sistemas Computacionais

Aula 02

Auditoria de Computadores

Aula 2

A Auditoria de Computadores

Nomenclatura Importante
Que iremos utilizar no decorrer do curso

PED – Processamento Eletrônico de Dados
ASI – Auditoria de Sistemas de Informação

Aula 2

A Auditoria de Computadores

A área de Auditora de Processamento Eletrônico de Dados (PED) compreende terminologia, conceituação e técnicas de três áreas distintas de conhecimento:

- auditoria
- sistemas de informações
- processamento eletrônico de dados

Outras áreas do conhecimento humano contribuem para a execução de uma auditoria de computador, mas as três áreas citadas formam a base.

A auditoria de sistemas de informações computadorizados varre, interliga-se e permeia as três áreas do conhecimento que lhe servem de base.

A área de Processamento Eletrônico de Dados é aquela que começa com os conceitos de hardware e de software e cresce enlaçando-se com a área de telecomunicações, criando ambientes altamente sofisticados e abrangentes de atuação.

Aula 2

Composição da estrutura da área de Processamento Eletrônico de Dados:

• **Hardware:** compreende dispositivos e equipamentos que compõem uma configuração de computador (unidade central de processamento, unidade de disco magnético, cabos de conexão de periféricos e dispositivos de computação, terminais impressoras, entre outros);

• **Software básico:** conjunto de instruções e programas de computador que cumprem as funções básicas de acionamento e controle do computador. Algumas vezes essas instruções são incorporadas as próprio hardware, gerando o conceito firmware.

• **Software de apoio:** conjunto de instruções e programas de computador que cumprem funções de uso freqüente e que podem ser padronizados para rapidez de acesso e uso. (programas utilitários, gerenciadores de banco de dados, monitores de comunicação).

Aula 2

Composição da estrutura da área de Processamento Eletrônico de Dados (continuação)

• **Software aplicativo:** conjunto de instruções e programas escritos pelos programadores ou usuários de computação para a conversão do dado da informação, com a conseqüente solução do problema que enfrentam.

• **Teleprocessamento:** entrelaçamento da área de computação com a área de telecomunicações, permitindo a conexão de equipamentos de processamento eletrônico de dados localizados a grandes distâncias físicas. Permite que a área de computação atinja um espaço geográfico ilimitado e que a tecnologia de computadores se torne fisicamente presente nas mãos dos usuários.

A área de Sistemas de Informações corresponde a todos os processos exercidos e resultados apurados, segundo objetivos e necessidades operacionais do ser humano.

Aula 2

Os sistemas de informação fazem parte da vida intelectual do homem, e existem para servi-lo. Entretanto, necessitamos caracterizar sistemas de informações e, por isso, vamos utilizar a definição a seguir:

"Sistemas de informações compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros, combinados segundo uma seqüência lógica para transformar dados em informações."

Aula 2

No ambiente de auditoria de computadores podemos detalhar da seguinte forma essa definição:

- recursos humanos compreendem os usuários dos sistemas computadorizados (funcionários da área administrativa, da área de vendas ou da área industrial), os profissionais de computação (operadores de computador, analistas de sistemas, programadores, fitotecários,...)
- recursos materiais tanto abrangem suprimentos (disquetes, formulários contínuos,...) quanto equipamentos (terminais, unidade central de processamento, impressoras,...) quanto instalações e utensílios (sala de operação, rede de energia elétrica, móveis,...)
- recursos tecnológicos correspondem ao intangível dos sistemas de informações, ou seja, são os softwares (programas de computador) e as informações geradas. É importante destacar que os recursos tecnológicos vivem agregados a recursos humanos e a recursos materiais.

7 Prof. Cláudio F. Rossoni

Aula 2

No ambiente de auditoria de computadores podemos detalhar da seguinte forma essa definição (continuação):

- recurso financeiro é a transformação dos recursos humanos, materiais e tecnológicos, segundo o denominador comum moeda
- a seqüência lógica exprime a idéia de dinamismo e compreende as tarefas ou atividades a serem cumpridas para a transformação do dado em informação. Corresponde, portanto, ao processo que é, por sua vez, um elenco de procedimentos manuais ou computadorizados (instruções de computador formando programas)
- os dados e as informações são estáticos e são os resultados – inicial e final – dos processos executados.

8 Prof. Cláudio F. Rossoni

Aula 2

No ambiente de auditoria de computadores podemos detalhar da seguinte forma essa definição (continuação):

Tanto processos quanto resultados são intangíveis e, portanto, correspondem a recursos tecnológicos que, para serem acionados, necessitam estar agregados a recursos humanos e a recursos materiais.

A área de auditoria implica a validação e avaliação do controle interno de sistemas de informações em processamento eletrônico de dados.

9 Prof. Cláudio F. Rossoni

Aula 2

O controle interno corresponde ao exercício de um ou mais dos seguintes parâmetros:

- **Fidelidade da informação em relação ao dado:** deve o auditor de sistemas validar e avaliar que informações criadas por um sistema de informações computadorizado, são corretas em relação ao dados alimentadas por esse mesmo sistema. Em outras palavras, o auditor deve certificar-se de que não foram inseridos nem perdidos dados ou informações semi-elaboradas durante o processo de transformação do dado em informação.
- **Segurança física:** corresponde à constatação de bom estado operacional dos recursos humanos (condições de saúde, ergonomia, sistema de proteção) e dos recursos materiais (instalações, hardware, suprimentos) que compõem e dão sustentação aos sistemas de informações computadorizadas.
- **Segurança lógica:** diz respeito a alterações, modificações ou erros dos recursos tecnológicos (processo e resultados) componentes de certo sistema de informação computadorizado.

Aula 2

O controle interno corresponde ao exercício de um ou mais dos seguintes parâmetros (continuação):

- **Confidencialidade:** compreende a quebra do sigilo do sistema computadorizado, seu processo e informações. É a captação, por entidade não autorizada, dos recursos tecnológicos componentes do ambiente computacional. Essa entidade não autorizada pode ser um recurso humano ou um recurso tecnológico.
- **Segurança ambiental:** implica a validação e avaliação das condições de operacionalidade dos recursos humanos, materiais e tecnológicos componentes da infra-estrutura do centro de computação.
- **Obediência à legislação em vigor:** é o atendimento pelos sistemas de informações computadorizados à legislação federal, estadual e municipal.
- **Eficiência:** é a combinação ótima dos recursos humanos, materiais e tecnológicos, impondo a melhor relação benefício versus custo aos processos computadorizados.

Aula 2

O controle interno corresponde ao exercício de um ou mais dos seguintes parâmetros (continuação):

- **Eficácia:** abrange a avaliação do nível de satisfação do usuário do sistema computadorizado. Avalia-se a informação foi gerada segundo os objetivos que determinam sua utilidade.
- **Obediência às políticas da alta administração:** consiste em verificar se o sistema computadorizado atende às normas vigentes, às diretrizes e políticas para a organização traçadas pela alta administração.

Aula 2

É importante notar que os parâmetros apresentados retratam a definição de controle interno do AICPA – American Institute of Certified Public Accountants – e traduzida pela IBRACON – Instituto Brasileiro de Contadores do Brasil.

A caracterização do AICPA e IBRACON estabelece ainda que o controle interno é dividido em dois subconjuntos:

- controle interno contábil
  - Fidelidade da informação em relação ao dado
  - Segurança física
  - Segurança lógica
  - Confidencialidade
  - Segurança ambiental
  - Obediência à legislação em vigor
- controle interno administrativo
  - Eficiência
  - Eficácia
  - Obediência às políticas da alta administração

13 Prof. Cláudio F. Rossoni

Aula 2

Utilizar metodologia em que a definição de sistemas de informações e de controle interno facilitam a elaboração de papéis de trabalho, o uso de matrizes, a administração da qualidade da auditoria de sistemas e a análise de risco a ser feita.

Dessa forma, as palavras-chave para uma adequada auditoria de computador são:

- recurso humanos;
- recurso material;
- recurso tecnológico;
- recurso financeiro;
- dados;
- informações;
- seqüência lógica;
- fidelidade da informação em relação ao dado;
- segurança física;
- segurança lógica;
- segurança ambiental;
- confidencialidade;
- obediência à legislação em vigor;
- eficiência e eficácia;
- obediência às políticas da alta administração;

14 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação

A auditoria de computador pode ocorrer:

- via sistema de informação computadorizado ou centro de computação;
- em nível de processo ou de resultados.

Quando atuamos via sistema computadorizado, temos como primeira tarefa retratar o fluxo do sistema e para tal temos usado a técnica de Diagrama de Fluxo de Dados (D.F.D.)

Na atuação via centro de computação necessitamos do layout da instalação física, da estrutura orgânica e das normas administrativas, técnicas e operacionais vigentes.

15 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Os trabalhos de auditoria desenvolvidos versus sistema computadorizado contemplam os parâmetros de controle interno:

- fidelidade da informação em relação ao dado;
- segurança física;
- segurança lógica;
- confidencialidade;
- obediência à legislação;
- eficiência;
- eficácia;
- obediência às políticas da alta administração.

16 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Os trabalhos de auditoria do centro de computação contemplam os parâmetros:

- segurança ambiental;
- obediência à legislação;
- eficiência;
- eficácia;
- obediência às políticas da alta administração.

Na realidade, o parâmetro segurança ambiental contempla os parâmetros segurança física dos recursos humanos e materiais, segurança lógica quanto a erros, fraude, modificações de recursos tecnológicos e confidencialidade quanto a captação indevida de recursos tecnológicos, todos estes recursos componentes da infra-estrutura do centro de computação ou, então, de uso comum por diversos sistemas de informações aplicativos computadorizados.

17 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

O parâmetro fidelidade da informação em relação ao dado atende à necessidade de integridade do dado, isto porque precisamos, como auditores, garantir que todos os dados de que foram alimentados os sistemas computadorizados receberam tratamento pelos programas que compõem esse sistema computadorizado e, mais ainda, que durante o processo ocorrido não foram introduzidos outros dados ilegítimos ao sistema computadorizado sob auditoria.

O parâmetro fidelidade da informação casa-se adequadamente com o conceito de *audit-trail* ou trilha de auditoria, a qual estabelece a necessidade de, a partir das informações, podermos recompor os dados.

Para garantirmos a fidelidade da informação em relação ao dado, devemos criar o arquivo de informação de controle (AIC), o qual materializa o conceito de audit-trail em um sistema computadorizado.

A AIC deverá conter acumuladores que, por natureza de registro, permitam a monitorização, tanto imediata quando a posteriori, do processamento de todos os dados e só deles pelo sistema sob auditoria.

18 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

O parâmetro fidelidade da informação busca a veracidade do recurso tecnológico, enquanto o parâmetro segurança lógica busca a correção dos recursos tecnológicos.

A auditoria de computador em nível de processos trata com rotinas operacionais e com rotinas de controle e em nível de resultados trata com informações, registros, arquivos operacionais e de controle.

Processos ou rotinas operacionais são aqueles que efetivamente transformam os dados em informações. Assim, por exemplo, a rotina de cálculo do imposto de renda, a rotina de atualização de cadastro de funcionários estão dando tratamento aos dados e gerando informações que implicam a existência do sistema computadorizado de folha de pagamento.

Processos ou rotinas de controle são aqueles agregados aos processos operacionais e que os monitoram ou controlam, gerando informações de controle em função da natureza das informações operacionais criadas pelas rotinas operacionais.

19 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Em sistemas de informações computadorizados podemos caracterizar como rotinas de controle:

a) Rotinas de crítica que verificam a validade de informação operacionais e geram informações de controle, apontando a incorreção nessas informações operacionais. Exemplo: o código do produto que deveria ser numérico e foi submetido ao sistema com caracteres alfabéticos; outro exemplo são rotinas de controle que identificam informações operacionais ou de controle fora de limites, que é o caso de informações operacionais alimentadas no sistema fora do prazo ou de erros ocorridos no sistema e não corrigidos em tempo oportuno.

b) Rotinas de consistência que dão tratamento à não oportunidade de atuação de rotinas operacionais. Exemplo: listar a inclusão de um item no cadastro por impossibilidade de a operação ser feita, já que foi constatada pela rotina operacional a existência de um item idêntico no cadastro.

20 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Rotinas e informações operacionais:

Natureza do processo – resultado	Exemplos:
Rotina operacional	- Rotina de atualização do cadastro de itens em estoque. - Rotina de cálculo de saldo em estoque.
Informação operacional	- Informações do cadastro de estoque atualizado. - Informação do saldo de estoque.

21 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Rotinas e informações de controle:

Natureza do processo – resultado	Exemplos:
Rotina de controle	-Rotina de gravação ou impressão de tentativa de inclusão de item já existente no cadastro de estoque. - Rotina de verificação quanto ao fato de o saldo do item em estoque ser negativo.
Informação de controle	- Item a ser incluído, já existente no cadastro de estoques e listados no relatório de erros na atualização. - Item em estoque com saldo negativo e impresso em relatório de erros.

22 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

O Ponto de Controle → é a situação do ambiente computacional caracterizada pelo auditor como de interesse para a validação e avaliação.

Esta caracterização de ponto de controle expõe toda a abrangência do trabalho de auditoria de computador em face da independência de o auditor ser o responsável único pela determinação do que, como e com que objetivos auditar.

O objetivo da auditoria do ponto de controle tanto pode ser sob a ótica do parâmetro do controle interno - segurança lógica, eficiência, confidencialidade etc. - quanto sob a ótica da fraqueza passível de ser identificada - erro, falha, falta, omissão do procedimentos ou falta, erro, correção de resultados.

O ponto de controle necessita ser caracterizado e podemos estabelecer sua composição em termos de:

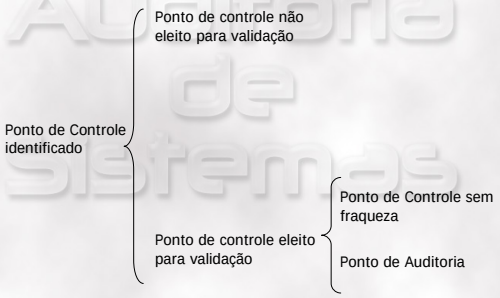
- uma combinação de rotinas e informações operacionais e de controle;
- recursos humanos, materiais e tecnológicos agrupados.

23 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Existe um ciclo de vida do ponto de controle estabelecido em termos de:



24 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

A auditoria de posição ocorre desde o momento em que o ponto de controle é identificado até o instante que, via avaliação dos resultados de sua validação, ele é determinado como apresentando fraqueza.

A auditoria de acompanhamento reflete as etapas e momentos em que, uma vez caracterizado a fraqueza do ponto de auditoria com o auditado, tornando o ponto de auditoria novamente ponto de controle.

Aula 2

Forma de atuação (continuação)

Para apoio à hierarquização dos pontos de controle com vistas no nível de interesse de sua avaliação ou de análise dos riscos potenciais que ocorre a organização, usamos os seguintes conceitos:

a) Walkthrough: (1)

- corresponde à representação gráfica de todo o ambiente computacional sob auditoria;
- mais uma vez, usamos o DFD para representar todos os processos e resultados operacionais e de controle de determinado sistema de informação;
- temos representado também, via DFD, o walkthrough da área de produção e a mecânica de desenvolvimento de sistemas, ou seja, a aplicação de uma metodologia de desenvolvimento de sistemas.

(1) (travessia – um esforço conjunto de revisão com a finalidade de melhorar a qualidade do produto em trabalhos de desenvolvimento de softwares)

Aula 2

Forma de atuação (continuação)

b) Walktruth:

- o caminho verdade, isto é, o conjunto de rotinas e informações operacionais mínimas e indispensáveis para a transformação do dado em informação.

c) Audit trail:

- o conjunto de rotinas e arquivos de controle que permitem, a partir das informações, reconstituirmos os dados.

d) Rotinas e resultados operacionais e de controle considerados não pertencentes ao Walktruth, nem ao Audit trail.

Aula 2

Forma de atuação (continuação)

É importante notar que o somatório de processos e resultados componentes dos itens Walktruth, Audit trail e Rotinas e resultados operacionais e de controle considerados não pertencentes ao Walktruth, nem ao Audit trail, deve ser igual à quantidade de processos e resultados que compõem o Walkthrough.

28 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

Classifica-se também o controle pela sua colocação dentro da seqüência de tempo em que ocorre um processo. Assim podemos ter:

1. Pré-conceito:
   - Rotinas e resultados embutidos e obtidos no início de um processamento, com o objetivo de garantir às rotinas operacionais a qualidade dos dados de que elas são alimentadas;
   - O programa de crítica e as primeiras rotinas de controle do programa de atualização são parte integrante do segmento de pré-controle;
   - A monitoração do erro via Arquivo de erros pendentes é das principais peças do pré-conceito.

29 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

2. Controle corrente:
   - Rotinas e informações de controle que acompanham o processamento ou que validam e dão o aval às informações operacionais geradas a cada seqüência de rotinas operacionais, concordando que as rotinas operacionais subseqüentes continuem a dar tratamento às informações operacionais semi-elaboradas;
   - O arquivo de informações de controle (AIC) e os arquivos estatísticos de acompanhamento de informações no limite do erro, as rotinas de verificação de informações operacionais negativas ou dentro de limites estabelecidos em tabelas, todos são exemplos de recursos tecnológicos componentes do controle corrente.

30 Prof. Cláudio F. Rossoni

Aula 2

Forma de atuação (continuação)

3. Pós-controle:
   - São rotinas que fazem cruzamento entre diversas informações operacionais finais geradas, ou entre informações finais e informações iniciais;

Como foi visto, o controle interno atua por cima das rotinas e resultados operacionais e de controle. Realmente, o controle sempre pressupõe um planejamento, mesmo que seja um padrão arbitrado. A auditoria de sistemas, valendo-se de sua função administrativa de controle interno, atua prioritariamente na validação da função administrativa de controle, voltando-se subsequentemente para as funções administrativas de execução e planejamento.

31 Prof. Cláudio F. Rossoni

Termino da Aula 2

32 Prof. Cláudio F. Rossoni